Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of digitally signing a plaintext message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key *a* and a public key derived from the private key *a* and available to the other of said pair of correspondents, said method comprising the steps of:

subdividing said plaintext message into a ~~pair of bit strings,~~ first plaintext bit string H and a second plaintext bit string V;

utilizing ~~one of said bit strings~~ said first plaintext bitstring H to compute a first signature component *c*, in which the plaintext is hidden;

forming from said first signature component *c* and ~~another of said bit strings~~ said second plaintext bit string V, an intermediate signature component *c'*[[,]];

utilizing said intermediate signature component *c'* and said private key *a* to provide a second signature component *s*, in which the plaintext is hidden; and

~~combining said first and second components with said other of said bit strings to provide a signature.~~ forming a signature (s,c,V) by including said first signature component *c*, said second signature component *s*, and said second plaintext bit string V as discrete signature components;

whereby during verification, said second plaintext bit string V is available as an input to a verification protocol.

2. (currently amended) A method according to claim 1 wherein redundancy in said ~~one of said bit strings~~ first plaintext bit string H is compared to a predetermined level prior to computing said first signature component *c*.

3. (previously presented) A method according to claim 2 wherein said redundancy is adjusted to exceed a predetermined level.

4. (currently amended) A method according to claim 3 wherein data is added to said ~~one of said~~

~~bit strings~~ first plaintext bit string H to adjust said redundancy.

5. (currently amended) A method according to claim 4 wherein an indicator is included in said ~~one of said bit strings~~ first plaintext bit string H to indicate ~~the data added~~ additional data.

6. (currently amended) A method according to claim 1 wherein said second signature component *s* is generated by hashing said first signature component *c* and said ~~other~~ second plaintext bit string V.

7. (currently amended) A method of verifying a plaintext message from a signature of a purported signer, said plaintext message being subdivided into a ~~pair of bit strings from a signature of a purported signer~~ first plaintext bit string H and a second plaintext bit string V, said signature formed as a set of discrete components, said components including at least one component having only ~~one of said bit strings~~ said first plaintext bit string H encrypted therein[[,]] and ~~the other of said bit strings,~~ a second component being said second plaintext bit string V, said purported signer having a private key used in the computation of said signature and a corresponding public key available for use in verification, said method comprising the steps of:

combining said one component with ~~the other of said bit strings,~~ said second plaintext bit string V;

recovering said ~~one of said bit strings~~ first plaintext bit string H from said combination using publicly available information of the purported signer including said public key; and

examining said recovered ~~one of said bit strings~~ first plaintext bit string H for a predetermined characteristic.

8. (currently amended) A method according to claim 7 wherein said combination of said one component and said ~~other~~ second plaintext bit string V includes hashing a combination of said one component and said ~~other of said bit strings.~~ second plaintext bit string V.

9. (currently amended) A method according to claim [[8]] 7 wherein said predetermined characteristic is the redundancy of said recovered ~~one~~ first plaintext bit string H.

10. (currently amended) A method according to claim 9 wherein said signature includes a ~~second~~ third component derived from a combination of said one component and said ~~other of said bit strings~~ second plaintext bit string V and said ~~one of said bit strings~~ first plaintext bit string H is recovered utilising said ~~second~~ third component.

11. (currently amended) A method according to claim 1 wherein said first signature component *c* is formed by applying a function to said ~~one of said bit strings~~ first plaintext bit string H and said ~~one of said bit strings~~ first plaintext bit string H may be recovered from said first signature component *c* by applying a complementary function to said first signature component *c*.

12. (previously presented) A method according to claim 11 wherein said function is encryption with a key, said key is recoverable from said signature, and said complementary function is decryption with said key.

13. (previously presented) A method according to claim 12, wherein said key is a short-term public key derived from a short-term private key used in the provision of said second signature component.